5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik

Voelsen, Daniel

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Voelsen, D. (2019). *5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik.* (SWP-Aktuell, 5/2019). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2019A05

SWP

SWP-Aktuell

NR. 5 FEBRUAR 2019

5G, Huawei und die Sicherheit unserer Kommunikationsnetze

Handlungsoptionen für die deutsche Politik

Daniel Voelsen

Die geplante Einführung des neuen Mobilfunkstandards 5G hat eine Debatte über die Sicherheit digitaler Kommunikationsnetze ausgelöst. Im Fokus steht dabei die Frage, ob westliche Staaten die Netzwerktechnologie des chinesischen Unternehmens Huawei nutzen sollten. Die USA und ihre engsten Verbündeten aus der Nachrichtendienstallianz »Five Eyes« sehen hierin ein erhebliches Sicherheitsrisiko und den Versuch Pekings, Einfluss auf die digitale Infrastruktur westlicher Staaten zu gewinnen. Sie drängen daher darauf, Huawei vom Aufbau der 5G-Mobilfunknetze auszuschließen. Dabei zeigt sich, dass die Kontroverse um Huawei eine im engeren Sinne technische Dimension hat, zugleich aber auch wirtschaftliche und geopolitische Interessen berührt. Mit Blick auf die anstehende Versteigerung der 5G-Lizenzen ergeben sich für die deutsche Politik verschiedene Optionen, sich zu dieser Kontroverse zu verhalten.

Seit dem letzten Jahr häufen sich die Warnungen vor einer Verwendung der Netzwerktechnologie des chinesischen Unternehmens Huawei.

Es sind vor allem die USA und ihre Verbündeten in der Nachrichtendienstallianz »Five Eyes« (Australien, Großbritannien, Kanada, Neuseeland), die eindringlich auf das Risiko hinweisen, dass Huawei chinesischen Sicherheitsbehörden unbemerkt Zugriff auf die Netze seiner Kunden ermöglichen könnte.

Die »Five Eyes« haben dabei das gesamte Spektrum an Netzwerktechnologie im Blick. So hat etwa Australien 2018 verhindert, dass Huawei den Auftrag für die Verlegung eines Unterseekabels erhält, das die Salomon-Inseln mit Australien verbinden soll. Auch die British Telecom hat nach eigenen Angaben damit begonnen, alle Produkte von Huawei aus dem Kern der schon bestehenden 3G- und 4G-Netze durch Produkte anderer Hersteller zu ersetzen.

Im Fokus der gegenwärtigen Debatte über Huawei steht aber der Aufbau von 5G-Netzen. Einige der hierfür unverzichtbaren Komponenten werden weltweit nahezu ausschließlich von drei Unternehmen angeboten: von Ericsson, Nokia und Huawei. Vor allem die USA und Australien drängen dennoch nachdrücklich darauf, die Produkte von Huawei zu meiden.

Einen vorläufigen Höhepunkt in dieser Konfrontation bildet die Verhaftung des

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Finanzvorstands von Huawei, Meng Wanzhou, in Kanada Anfang Dezember. Dass kurz darauf ein Kanadier in China wegen Drogenschmuggels zum Tode verurteilt wurde, werten viele Beobachter als Vergeltungsmaßnahme Pekings.

Mittlerweile hat die Konfrontation auch Europa erreicht. Im Januar dieses Jahres wurde in Polen ein Mitarbeiter von Huawei unter dem Vorwurf der Spionage verhaftet. Die polnische Regierung nahm den Fall zum Anlass, ein gemeinsames Vorgehen der Nato und der EU gegen Huawei zu fordern.

Huawei selbst bestreitet den Vorwurf der Zusammenarbeit mit den chinesischen Sicherheitsbehörden. Und auch in Deutschland ist man bisher nicht willens, sich der Kritik der »Five Eyes« anzuschließen. Die Betreiber der deutschen Mobilfunknetze — Telekom, Vodafone und Telefónica — nutzen schon seit einigen Jahren Produkte von Huawei. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Dezember noch einmal bekräftigt, dass nach eingehender Prüfung keinerlei Hinweise auf Vorkehrungen zu Spionagezwecken gefunden worden seien. Zwar wird beim Betrieb des deutschen Regierungsnetzwerks (IVBB) bewusst auf Komponenten aus China verzichtet, bisher ist jedoch nicht geplant, deutschen Netzbetreibern entsprechende Vorgaben zu machen.

Mit Blick auf die anstehenden Versteigerungen der Lizenzen für 5G-Frequenzen wächst jedoch der Druck auf die deutsche Politik, ihre Position zur Sicherheit der Mobilfunknetze zu erläutern. Konkret wird die Bundesregierung dazu Stellung beziehen müssen, ob beim Aufbau von 5G-Netzen Technologie von Huawei zulässig sein soll.

Die technische Dimension: Zur Sicherheit von 5G-Netzen

Ein durchaus positiver Effekt der aktuellen Kontroverse um Huawei liegt darin, dass sie das öffentliche Interesse an der Sicherheit von Netzwerktechnologie deutlich gesteigert hat.

Von der öffentlichen Verwaltung über die Wirtschaft bis weit in das Privatleben hinein sind moderne Gesellschaften immer mehr auf internetbasierte Kommunikation angewiesen. Netzwerktechnologie ist ein wesentliches Element der hierfür notwendigen technischen Infrastruktur. Sie ist somit selbst Teil der kritischen Infrastruktur und zudem Voraussetzung für den Betrieb der technischen Infrastruktur in vielen weiteren besonders kritischen Bereichen, etwa für den Betrieb der Stromnetze.

Die Kontroverse um 5G dreht sich um eine maßgebliche Komponente dieser Infrastruktur. In der Tat zeichnet sich schon heute ab, dass der Zugang über Mobilfunknetze immer mehr an Bedeutung gewinnen wird. Der neue Mobilfunkstandard 5G ist explizit darauf ausgelegt, im Sinne der Vision eines »Internets der Dinge« immer mehr Geräte mit dem Internet zu verbinden und dabei je nach Bedarf hohe Übertragungsgeschwindigkeiten, niedrige Verzögerungen beim Verbindungsaufbau (Latenz) oder auch die Nutzung in Kleinstsensoren mit geringem Stromverbrauch zu ermöglichen. So soll 5G die Basis für jenen intensiven Datenaustausch legen, der als Voraussetzung für autonomes Fahren und die Digitalisierung von industriellen Produktionsprozessen (»Industrie 4.0«) gilt (vgl. SWP-Aktuell 41/2018).

Die neuen Möglichkeiten von 5G haben Auswirkungen auch auf die Architektur der entsprechenden Mobilfunknetzwerke. Für die Diskussion über die Sicherheit der 5G-Netze sind dabei vor allem zwei Faktoren entscheidend:

Erstens ist es eine der wesentlichen Neuerungen von 5G, dass das Mobilfunknetzwerk deutlich stärker als früher »virtualisiert«, also per Software ausgestaltet wird. Dies soll es erlauben, das Netzwerk dynamisch den jeweiligen Nutzungsanforderungen anzupassen. Die Folge ist, dass es bei 5G nicht möglich ist, mit Blick auf die eingesetzte Technologie klar zwischen Hard- und Software zu unterscheiden. Im Gegenteil, die Produkte aller 5G-Netzwerkausrüster sind immer spezifische Kombinationen von Hard- und Software.

Zweitens erfordert die Feinsteuerung der Datenströme im Rahmen von 5G eine stärkere Integration des Netzwerks, als dies bei früheren Mobilfunkstandards der Fall war. Grob vereinfacht lässt sich bei Mobilfunknetzen zwischen den »Radio Access Networks« (RAN) und den »Core Networks« unterscheiden. Die RAN dienen im Wesentlichen dazu, die Endgeräte per Funksignal mit den Antennenmasten zu verbinden; von dort werden die Daten dann an das »Core Network« weitergeleitet, wo die weitere Datenübermittlung gesteuert wird. Entscheidend ist nun, dass sich die besonderen Eigenschaften von 5G-Netzwerken nicht allein im »Core Network« realisieren lassen, sondern dafür schon beim RAN angesetzt werden muss. Dies verschärft die Diskussion um Huawei nochmals: Im Falle von 3G- und 4G-Netzen ist es für ein Unternehmen wie die British Telecom noch möglich, Huawei im »Core Network« auszuschließen und dennoch weiter RAN-Produkte der Firma zu nutzen. Bei 5G hingegen ist diese Aufteilung nicht mehr realisierbar. Schon über das RAN erhielte Huawei weitreichenden Zugriff auf das Netzwerk.

Die Sorge vor Spionage

In der Debatte um Huawei wird immer wieder die Sorge laut, das Unternehmen könnte in seinen 5G-Produkten *backdoors* einrichten, also technische Hintertüren, die chinesischen Sicherheitsbehörden einen Zugriff auf Daten erlauben würden.

Die Rede von *backdoors* ist in diesem Fall allerdings irreführend. Bei Netzwerktechnologie handelt es sich um komplexe technische Systeme. Alle Anbieter in diesem Bereich konfigurieren ihre Produkte daher so, dass eine Fernwartung möglich ist. Die entscheidende Frage ist somit nicht, ob ein solcher Zugang besteht, sondern ob er über die Fernwartung hinaus auch für Spionagezwecke genutzt werden kann.

Es ist schwer vorstellbar, dass auf diese Weise unbemerkt alle Daten, die über ein Netz laufen, an Unbefugte weitergeleitet werden könnten. Das entsprechende Datenvolumen wäre enorm und entsprechend auffällig. Plausibler ist das Risiko, dass über den Fernwartungszugang Daten gezielt etwa nach Datentyp, Absender oder Empfänger gefiltert werden; die entsprechenden Datenmengen würden in großen Netzwerken wahrscheinlich keine Aufmerksamkeit erregen. Auf diese Weise ließe sich tatsächlich politische oder wirtschaftlich motivierte Spionage betreiben. In der Tat war es die Sorge vor ebendieser Art von Spionage, die die Bundesregierung nach den Snowden-Enthüllungen dazu gebracht hat, im Netz der Regierung und des Bundestags nicht länger Produkte des US-Unternehmens Verizon zu verwenden.

Um festzustellen, ob Netzwerkprodukte für diese Art von gezielter Spionage genutzt werden, gibt es zwei Ansätze, die jedoch beide nur begrenzte Aussagekraft haben. Zum einen prüft das BSI schon seit längerem den Programmcode der Produkte von Firmen wie Huawei und Cisco (»code inspection«). Problematisch dabei ist allerdings, dass dies immer nur Momentaufnahmen sind. Über den Fernzugriff haben die Unternehmen jederzeit die Möglichkeit, den Programmcode zu ändern. Um per »code inspection« sichere Aussagen über die Verwendung der eingesetzten Produkte treffen zu können, wäre es nötig, jede Änderung des Programmcodes zu erfassen und zeitnah auszuwerten. Dies geschieht in Deutschland bisher nicht. Bemerkenswert ist in diesem Kontext eine 2018 veröffentlichte Einschätzung des britischen Government Communications Headquarters (GCHQ): Man habe zwar den von Huawei zur Verfügung gestellten Programmcode geprüft, könne aber keine zuverlässigen Aussagen über jenen Programmcode treffen, der in den Produkten von Huawei tatsächlich zur Anwendung kommt.

Jenseits der Überprüfung des Programmcodes gibt es zum anderen die Möglichkeit, im realen Betrieb zu beobachten, welche Daten die Produkte von Huawei über den Fernwartungskanal senden. Zum Teil findet dies bereits standardisiert statt und so würde, wie oben beschrieben, auffallen, wenn auf diese Weise große Datenmengen abflössen. Kleine Datenvolumen jedoch würden kaum

bemerkt werden. Da diese Verbindungen zudem üblicherweise verschlüsselt sind, wären gezielte Spionageaktivitäten auf diese Weise nicht zu identifizieren.

Die Gefahr, dass über Netzwerktechnologie Möglichkeiten der Spionage geschaffen werden, ist mithin real. Auch gibt es bisher keine zuverlässigen Prüfverfahren, um dies auszuschließen.

Allerdings gilt es auch zu bedenken, dass es für ebendiese Zwecke eine Reihe weiterer technischer Zugriffsmöglichkeiten gibt. Weit verbreitet ist etwa die Praxis, dass Staaten an Internet-Knotenpunkten (IXPs) in großem Umfang Daten sammeln. Ebenso üblich ist es, dass Staaten von Unternehmen verlangen, ihnen im Rahmen der Strafverfolgung Daten der eigenen Bürger wie auch Bürger anderer Staaten zur Verfügung zu stellen. Besonders weit geht hier der US-amerikanische *Patriot Act*, der über die Strafverfolgung hinaus in den USA ansässige Firmen zur Zusammenarbeit mit Sicherheitsbehörden verpflichtet. Darüber hinaus nutzen immer mehr Staaten verschiedene Techniken, um sich direkten Zugriff auf Server oder Endgeräte zu verschaffen.

»kill switch« – Die Sorge vor gezielten Störungen der Netze

Hinzu kommt schließlich noch eine gänzlich anders gelagerte Gefahr, nämlich die der gezielten Störung von Mobilfunknetzen. Technisch denkbar ist etwa, dass die Verfügbarkeit von einzelnen Teilnetzen eingeschränkt wird, um zum Beispiel Produktionsprozesse in der Industrie oder die Steuerung der Energieversorgung zu stören.

Indes ist es unwahrscheinlich, dass ein Unternehmen wie Huawei von dieser Möglichkeit flächendeckend Gebrauch macht. Die negativen Konsequenzen für das Unternehmen selbst, wie auch für die chinesische Regierung, wären enorm. Eine solch umfassende Störung ist daher allenfalls im Falle massiver zwischenstaatlicher Auseinandersetzungen vorstellbar.

Bedenkt man allerdings, dass 5G explizit dazu dienen soll, immer mehr Geräte und gerade auch industrielle Produktionsprozesse über das Mobilfunknetz zu verbinden, so wäre durchaus vorstellbar, dass schon kleine Störungen der Verfügbarkeit des 5G-Netzwerks erhebliche Konsequenzen haben könnten. Zugleich könnten solche Vorfälle hinreichend plausibel als Folge unbeabsichtigter Fehler dargestellt werden.

Die wirtschaftliche Dimension: Privatisierung von Infrastruktur und Marktkonzentration

In den meisten westlichen Staaten werden Kabel- und Mobilfunknetze seit der Privatisierung vormals staatlicher Telekommunikationsbehörden in den 1990er Jahren von privaten Unternehmen betrieben.

Dahinter steht bis heute die Erwartung, dass Unternehmen aus eigenem wirtschaftlichem Interesse zuverlässige und innovative Dienstleistungen anbieten. Immer deutlicher zeigt sich allerdings, dass die Interessen der Mobilfunkbetreiber nicht in allen Fällen mit denen der Staaten einhergehen. Die Bereitstellung von Netzzugängen in dünn besiedelten Räumen etwa ist für die Firmen wirtschaftlich unattraktiv, gilt vielen Staaten aber als wichtige Maßnahme zur Förderung solcher Regionen. Die Staaten versuchen dementsprechend, die Vergabe von Lizenzen an politische Vorgaben zu knüpfen, wie aktuell in Deutschland im Fall der 5G-Lizenzen zu beobachten ist.

Die privatwirtschaftliche Bereitstellung der Internet-Infrastruktur hat des Weiteren den erwartbaren und politisch gewünschten Effekt, dass die Unternehmen sich beim Einkauf der benötigten Technologie primär an ökonomischen Kriterien orientieren. Die Förderung der nationalen Industrie oder strategische staatliche Interessen spielen bei diesen Entscheidungen der Unternehmen daher allenfalls eine sehr geringe Rolle.

Auch Sicherheitserwägungen haben auf Seiten der Firmen nur einen nachrangigen Stellenwert: Zwar haben die Betreiber der Netzwerke ein Eigeninteresse an sicherer Technologie, um etwa die missbräuchliche Nutzung ihrer Infrastruktur oder deren Ausfall zu vermeiden. Auch will sich kein

Unternehmen vorwerfen lassen müssen, jene Sicherheitsmindeststandards nicht zu erfüllen, die das Telekommunikationsgesetz gebietet. Über das gesetzlich geforderte Mindestmaß hinaus jedoch gibt es kaum Anreize für die Unternehmen, Investitionen in Sicherheitsmaßnahmen vorzunehmen, die den wenigsten Endverbrauchern erklärlich sind und für die diese wohl auch nicht bereit wären, höhere Preise zu zahlen.

Hinzu kommt, dass es auf dem spezialisierten Markt für Netzwerktechnologie eine starke Konzentration gibt. Dies gilt in besonderer Weise für die »Radio Access Networks« (RAN). RANs für 5G-Netze werden derzeit auf dem globalen Markt im Wesentlichen von drei Firmen angeboten: neben Huawei sind dies Ericsson aus Schweden und Nokia aus Finnland. Das ebenfalls chinesische Unternehmen ZTE bietet entsprechende Produkte nur innerhalb Chinas an; der südkoreanische Konzern Samsung bemüht sich mit erheblichen Investitionen, in diesen Markt einzusteigen, und profitiert dabei von den Erfahrungen beim Aufbau des 5G-Netzwerks in seinem Stammland.

Produkte im Bereich der 5G-»Core Networks« werden neben diesen Firmen von einer Reihe weiterer Unternehmen angeboten. Unter anderem arbeitet auch Cisco aus den USA an entsprechenden Komponenten (wobei seit Jahren gerade in den Produkten von Cisco immer wieder nicht dokumentierte *backdoors* gefunden werden). Geht man wie beschrieben davon aus, dass bei 5G-Netzen RAN und »Core Network« eng aufeinander abgestimmt sein müssen, so ist die Auswahl für die Netzwerkbetreiber gleichwohl erheblich eingeschränkt. Letztlich sind sie angewiesen auf jenen kleinen Kreis von Unternehmen, die 5G-RANs anbieten.

Die geopolitische Dimension: USA vs. China

Erschwerend kommt hinzu, dass die aktuelle Diskussion über die Sicherheit der Netzwerktechnologie von einem geopolitischen Konflikt durchdrungen ist. Politikwissenschaftlich betrachtet ist die Deutung (das »framing«) eines Konflikts als geopolitisch selbst schon ein politisches Konstrukt. Wenn sich aber mächtige Akteure wie China und die USA eine solche Deutung zu eigen machen, wird diese zu einer Realität, der sich die deutsche Politik stellen muss.

Sowohl China als auch die USA und deren Verbündete aus der Nachrichtendienstallianz »Five Eyes« haben ein Interesse daran, ihre Möglichkeiten der digitalen Informationsgewinnung auszubauen. Im Falle der »Five Eyes« haben wir dank der Snowden-Enthüllungen zumindest einen gewissen Einblick in das Ausmaß der darauf ausgerichteten Aktivitäten, wenngleich hierzu keine aktuellen Informationen vorliegen. Bemerkenswert ist aber doch, dass die »Five Eyes« im September 2018 noch einmal gemeinsam die Forderung erhoben haben, dass Telekommunikationsfirmen in ihrem Einflussbereich ihnen die Möglichkeit einräumen müssten, die Verschlüsselung der von den Unternehmen angebotenen Dienste zu umgehen (»lawful access«). Bedenkt man, wie weit verbreitet Hard- und Software insbesondere aus den USA ist, so wird deutlich, wie weit dieser Anspruch reicht.

Vor diesem Hintergrund erscheint es weniger spektakulär, dass auch die chinesische Regierung die Unternehmen in ihrem Einflussbereich auf die Zusammenarbeit mit den nationalen Sicherheitsbehörden verpflichtet. So heißt es sehr klar in Artikel 7 des chinesischen National Intelligence Law von 2017: »All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of« (unautorisierte Übersetzung).

Der Versuch der USA, Huawei aus westlichen Märkten zu verdrängen, ist mithin zunächst darauf gerichtet, chinesischen Sicherheitsbehörden eine Möglichkeit zur Spionage sowie zur gezielten Störung der Kommunikationsnetze zu nehmen. Dies lässt sich auch als eine präventive Maßnahme verstehen. Demnach wäre es nachrangig, ob die chinesische Regierung von dieser Möglichkeit in der Vergangenheit Gebrauch

gemacht hat oder dies für die unmittelbare Zukunft plant.

Darüber hinaus deutet aber vieles darauf hin, dass die »Five Eyes« und insbesondere die USA unter Trump dieser Auseinandersetzung auch eine grundsätzlichere geopolitische Bedeutung beimessen. Washington geht es nicht nur um den Schutz der eigenen Netze, sondern auch darum, chinesischen Unternehmen den Zugang zu den Netzen anderer Staaten zu verwehren. Auf der Ebene der technischen Infrastruktur soll so das Eindringen Chinas in jenen Bereich verhindert werden, der von den »Five Eyes« als eigene digitale Einflusssphäre beansprucht wird.

Ebenfalls spricht vieles dafür, dass auch China in dieser Frage geopolitische Interessen verfolgt. So finden sich im Rahmen der »One Belt, One Road«-Initiative und im Kontext der chinesischen Digitalstrategie immer wieder Hinweise darauf, dass China den Aufbau eigener Infrastrukturen von globaler Reichweite, und damit verbunden die Durchsetzung eigener Standards, sehr klar als Machtinstrument versteht (vgl. SWP-Aktuell 18/2018).

Die Durchsetzung wirtschaftlicher Interessen ist bei diesem geopolitischen Konflikt für beide Seiten zugleich Ziel und Mittel. Der globale Markt für Produkte zum Betrieb von Kommunikationsnetzwerken ist lukrativ und wird aller Voraussicht nach weiter wachsen. Dementsprechend ist es ein attraktives Ziel für Unternehmen, und auch Staaten, hier stark vertreten zu sein und globale Standards setzen zu können. Eine solche wirtschaftliche Dominanz in einem wichtigen technologischen Bereich kann zudem aber auch ein Mittel sein, um darüber hinausgehende Interessen zu verfolgen.

Im Fall der 5G-Technologie ist China mit Huawei und ZTE derzeit besonders gut aufgestellt, während gerade US-amerikanische Unternehmen hier noch Aufholbedarf haben. Ein Ausschluss von Huawei von westlichen Märkten hätte vor diesem Hintergrund nicht nur den unmittelbaren ökonomischen Effekt, die aktuellen Konkurrenten Nokia und Ericsson zu stärken, sondern würde mindestens mittelfristig auch US-Unternehmen neue Geschäftsmöglichkeiten eröffnen.

Handlungsoptionen für die deutsche Politik

Der Konflikt um Huawei wirft grundlegende Fragen zur Sicherheit von Netzwerktechnologie auf. An Brisanz gewinnen diese Fragen für die deutsche Politik dadurch, dass spätestens mit der für März geplanten Versteigerung der 5G-Lizenzen strategische Entscheidungen zum Aufbau des deutschen 5G-Netzes anstehen.

Sicherheit, Verfügbarkeit oder technologische Unabhängigkeit?

Um diese Entscheidungen zu treffen, ist es wichtig zu klären, welche Maßnahmen zum Erreichen welcher Ziele geeignet sind und mit welchen politischen und finanziellen Kosten diese Maßnahmen jeweils verbunden sind.

Ist das Ziel die Vermeidung von Spionage, so sollte Deutschland unabhängig von der Entscheidung für oder gegen Produkte von Huawei die bestehenden Möglichkeiten zur Verschlüsselung von Kommunikation bewahren und ausbauen. Richtig konfiguriert bietet eine Ende-zu-Ende-Verschlüsselung auf Anwendungsebene ein hohes Maß an Sicherheit, die für die Nutzer zudem transparent nachvollziehbar ist.

Neben der Verschlüsselung auf Anwendungsebene bietet es sich an, die spezifischen Features von 5G für ebendiese Zwecke zu nutzen. Wie beschrieben sind 5G-Netze darauf ausgelegt, im Rahmen einer physischen Infrastruktur Netzwerke in einzelne Einheiten (»slices«) virtuell aufzuteilen. Dies würde es auch erlauben, besonders sichere Verbindungswege zu gestalten und auch als solche zu vermarkten. Als weitere Sicherheitsmaßnahme ist dabei vorstellbar, dass die Bereitstellung derartiger »high security slices« nicht von den Netzwerkbetreibern selbst angeboten wird, sondern von Firmen, die sich darauf spezialisieren, ähnlich wie heute schon bei VPN-Verbindungen. Die

Frage, welches Unternehmen die Technik für die Netzwerkinfrastruktur stellt, würde so erheblich an Bedeutung verlieren.

Die genannten Maßnahmen zur Verschlüsselung würden das Spionagerisiko erheblich reduzieren. Selbst wenn über die Netzwerktechnologie von Huawei Daten abgegriffen werden würden, wären die Daten verschlüsselt und mithin unbrauchbar.

Nicht gebannt wäre damit allerdings die Gefahr, dass ein Unternehmen wie Huawei dazu gedrängt werden könnte, die Verfügbarkeit des 5G-Netzes gezielt zu stören. Um dieser Gefahr vorzubeugen, wäre es ratsam, redundante Kommunikationsstrukturen einzurichten bzw. zu erhalten. In vielen Regionen ist es heute üblich, dass sich die Netze der Mobilfunkanbieter überlappen. In ebendieser Weise wäre es möglich, mehrere technisch voneinander unabhängige 5G-Netze zu betreiben. Der flächendeckende und dauerhafte Betrieb solcher Parallelstrukturen würde gewisse Effizienzverluste und damit verbundene Mehrkosten mit sich bringen, dafür aber das Risiko von Netzwerkstörungen verringern. Es gibt mithin eine Reihe von technischen Maßnahmen, die geeignet sind, der Sorge vor Spionage und gezielten Störungen zu begegnen — und dies unabhängig davon, welches Unternehmen die Netzwerktechnologie stellt.

Die Debatte über den Umgang mit Huawei wirft aber darüber hinaus die Frage auf, wie die deutsche Politik vor dem Hintergrund der geopolitischen Auseinandersetzungen zwischen den USA und China die eigene technologische Unabhängigkeit gewichtet — und welchen Preis Deutschland hierfür zu zahlen bereit ist. Für die deutsche Politik zeichnen sich dabei drei Handlungsoptionen ab:

Option 1: Fortführung der bisherigen Politik

Eine Möglichkeit wäre, an der bisherigen Praxis festzuhalten, also den Netzwerkbetreibern zu erlauben, auch weiterhin Technologie von Huawei einzusetzen. Wie beschrieben ließe sich das Risiko der Spionage durch den Einsatz von Verschlüsselung reduzieren, der Gefahr gezielter Störungen der Verfügbarkeit des Netzes könnte durch den Aufbau redundanter Strukturen vorgebeugt werden. Auch könnte die Bundesregierung von Huawei finanzielle Sicherheiten verlangen und wie bisher die Produkte des Unternehmens regelmäßigen Kontrollen unterziehen. Schließlich könnte die Regierung dafür Sorge tragen, dass Technologie von Huawei nicht in besonders sensiblen Netzen eingesetzt wird. Im Regierungsnetzwerk ist dies schon heute so; entsprechende Vorgaben ließen sich auf andere Elemente der kritischen Infrastruktur ausweiten.

In wirtschaftlicher Hinsicht würde ein solches Vorgehen bedeuten, dass man an der bisherigen Politik der Privatisierung der Kommunikationsnetzwerke festhält. Aller Voraussicht nach würde Huawei in der Folge seine schon heute starke Stellung auf dem Markt für Netzwerktechnologie weiter ausbauen.

Im Hinblick auf die geopolitische Dimension der Huawei-Kontroverse würde diese Politik wahrscheinlich sowohl von den »Five Eyes« als auch von China selbst als Entgegenkommen Deutschlands gegenüber China gewertet. Will die deutsche Politik ein solches Signal vermeiden, müsste sie beiden Seiten deutlich machen, dass und warum die Entscheidung für Huawei nicht als geopolitische Positionierung zu verstehen ist.

Option 2: Schulterschluss mit den USA

Eine Alternative zur gegenwärtigen Politik Deutschlands bestünde darin, sich der Bewertung der »Five Eyes« anzuschließen und in Huawei ein Instrument chinesischer Geopolitik zu sehen. Dies würde es nahelegen, Huawei weitgehend vom Aufbau des 5G-Netzes auszuschließen.

Mit Blick auf die Sicherheit des 5G-Netzes wäre der chinesischen Regierung damit eine wichtige Möglichkeit zur Spionage und zur Störung der deutschen Mobilfunknetze genommen.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364
doi: 10.18449/2019A05

Die kurzfristige Alternative für die Netzwerkbetreiber bestünde darin, auf die Produkte von Nokia und Ericsson zurückzugreifen. Dies würde aller Voraussicht nach zu höheren Kosten führen. Ein Grund für die schnelle Ausbreitung von Huawei in den letzten Jahren war, dass das Unternehmen mit niedrigen Preisen locken konnte. Diese werden auf die geringen Produktionskosten in China und die gezielte Förderung Huaweis durch den chinesischen Staat zurückgeführt. Es ist nicht davon auszugehen, dass westliche Unternehmen ihre Produkte auf diesem Preisniveau anbieten können. Schließlich würde sich der Aufbau von 5G wahrscheinlich verzögern, weil die Konkurrenten erst entsprechende Produktionskapazitäten aufbauen müssten.

Mindestens mittelfristig würde der Ausschluss von Huawei aber auch Unternehmen wie Samsung und Cisco eine Chance bieten, sich auf dem deutschen 5G-Markt zu etablieren. Wie beschrieben bestünde insbesondere bei US-Unternehmen wie Cisco auch bei diesem Vorgehen die Gefahr, Opfer von Spionageaktivitäten zu werden. Eine bewusste Entscheidung für den Schulterschluss mit den USA allerdings würde implizieren, diesem Risiko weniger Gewicht zuzumessen.

In geopolitischer Hinsicht würde sich Deutschland mit diesem Vorgehen klar im westlichen Lager verorten. Wie China auf eine solch klare Positionierung reagieren würde, ist schwer abzusehen.

Option 3: Eine rein europäische Lösung

In einer noch weitergehenden Entscheidung könnte sich Deutschland darauf beschränken, beim Aufbau des 5G-Netzes nur Produkte von Firmen zu verwenden, die ihren Hauptsitz in Europa haben, aktuell also im Wesentlichen Nokia und Ericsson.

Geht man davon aus, dass Unternehmen mit Hauptsitz in Europa in besonderer Weise der Kontrolle durch europäische Institutionen unterstehen, so würde ein solches Vorgehen das Risiko von Spionage wie auch die Gefahr gezielter Störungen erheblich reduzieren. Dies würde sowohl im Verhältnis zu China als auch zu den »Five Eyes« gelten.

Die wirtschaftlichen Implikationen dieser Option wären ähnlich wie beim Schulterschluss mit den USA. Auch bei dieser Marschroute wäre damit zu rechnen, dass die Kosten für den Aufbau des 5G-Netzes steigen und sich dieser verzögern würde. Hinzu käme allerdings, dass bei einer strikt europäischen Lösung auch ein südkoreanischer Anbieter wie Samsung ausgeschlossen würde. Zu erwarten wäre im Umkehrschluss, dass dies europäischen Unternehmen zugutekäme.

In geopolitischer Hinsicht würde Deutschland damit seine Unabhängigkeit sowohl gegenüber China als auch gegenüber den USA festigen. Auch könnte eine solche Entscheidung dazu beitragen, die Rolle Europas in Fragen der Digitalpolitik zu stärken. Allerdings ist nach derzeitigem Stand unwahrscheinlich, dass sich die EU-Mitgliedsstaaten in dieser Frage auf ein einheitliches Vorgehen verständigen können. Vielmehr ist davon auszugehen, dass sich eine Reihe von Mitgliedsstaaten eher für den Schulterschluss mit den USA entschließen wird, andere hingegen die Beziehungen zu China nicht gefährden wollen.

Schließlich ist nicht abzusehen, ob und wie die USA darauf reagieren würden, dass ihren Unternehmen der Zugang zum deutschen Markt verwehrt wird.

Die drei skizzierten Handlungsoptionen zeigen auf, dass es bei der Kontroverse um 5G neben technischen Sicherheitserwägungen im engeren Sinne auch um wirtschaftliche und geopolitische Fragen von erheblicher Reichweite geht. Die anstehenden Entscheidungen zum Aufbau des 5G-Netzes erfordern mithin eine genuin politische Abwägung verschiedener Güter und Prioritäten. Insbesondere gilt es dabei zu klären, wie sich Deutschland in der geopolitischen Auseinandersetzung zwischen den USA und China positionieren will.

Dr. Daniel Voelsen ist Wissenschaftler in der Forschungsgruppe Globale Fragen.